SPPDT-Secure Privacy Preserving Data Transmission in Ad-Hoc Network

I. Varalakshmi
Asst Prof,Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Pondicherry,India

S. Jayamoorthy
Department of Computer Science and Engineering Manakula Vinayagar Institute of Technology, Pondicherry ,India

S. Kalaivani
Asst Prof,Department of Computer Science and Engineering,Manakula Vinayagar Institute of Technology, Pondicherry,India

Abstract—**The wireless technology plays major role in network communication and it is the most influential technological accomplishments in our daily lives in the form of mobile computing and wireless computing. MANET plays vital role in wireless network, because MANET carries large number of mobile nodes and produces topological changes and broadcast paradigm. For secure transmission, consider when the data transmitted within MANET, requires high degree of security. In this paper, provide a high degree of security when transmitting a data in wireless network. Based on Partition detection in distributed method, partition the nodes in MANET environment and identifies the failure occur in the network. Beacon frame contains the information about all the nodes in the Partition Detection Method (PDM) network, so that the fixed number of nodes are clustered into single group , because there are thousands of nodes participated in the wireless network for data transmission and it very difficult to identify if fault occurs, so that the partition method used. The sink node carries the router information along with the router table, the router table contains: Source, destination, Time period, Status, Distance/Cost. For transmitting the packets, should prefer only the shortest path, by using Distributed Bellman Ford algorithm (DBF) to find the shortest path from source to next hop. TTL assign time for every node, initially system allocated time and increased by secs, this technique is used to predict to be proving to failure. In the existing work, there are so many limitation using DSDV, AODV, DSR protocol, wastage of bandwidth, no efficiency, Message overhead occurs, Delay occurs. To overcome these parameters, the proposed system, design a protocol called Secure Privacy Preserving Data Transmission (SPPDT) in ad-hoc network is to prevent the node from attackers and predict the node status and recover the information, so that the information is kept secure and highly confidential.**

Keywords— DBF-DSV, SPPDT, PDM, Beacon Frame.

I. INTRODUCTION

In the initial state of communication, the datas are transmitted in wired network between the sender and receiver using TCP/IP protocol and its layers. The datas are shared between the institution, area and around the world using the network types like Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide Area Network(WAN)

The next generation/stage of this development is wireless technology. It is very difficult to transmit the packets in network using wired and it is very expensive and difficult to identify the problem occurred and rectified. For these cases, use wireless network. This become one of the most influential technological accomplishments and pervaded our daily lives in forms of mobile telephony and wireless computing. Due to the rapid development of technology and wide- spread applications, security and privacy issues in wireless network have become very important technique. In wireless, the most important issue is security, (i.e.) sensitive data and application are transmitted within the mobile ad hoc network and it requires high degree of security. The ad-hoc network has decentralized type of wireless network while because every node in a network can communicate with each other node present in a network with some kind of network topology or existence of resource usage.

In general, node to node communication can takes place through routing. Routing is defined as selecting the best and optimum shortest path among the alternatives. For selecting best path routing protocol such as Dijikistra, Krushkal‟s algorithm etc., These algorithms can helps to improve the quality of data delivery between end to end node. The routing table has maintained complete history of each and every node present in the network, because it maintains node status and their overall participation of other nodes present in a network. Even though routing table maintains history of all nodes present in a network, but particularly in ad-hoc network does not have any centralized node to update the status of particular node present in that zone.

In MANET, there is no centralized server, to monitor all the nodes which are participated in the network. The infrastructure services like routing, naming and the certification authorize of MANET differs highly from traditional wireless network. Routing in MANET is very challenging factors because, it has no infrastructure, no connectivity between the nodes, and here all are mobiles and open nature to overcome these issues/ limitations imposed by ad hoc network.The attacks in MANET can be classified into two categories, namely passive attacks and active attacks.

A **passive attack** obtains data exchanged in the network without disrupting the operation of the communications. A malicious node in the mobile ad hoc network executes a passive attack, without actively initiating malicious actions. The malicious node attempts to learn important information from the system by monitoring and listening on the communication between parties within the mobile ad hoc network.

An **active attack** involves information interruption, modification, or fabrication, thereby disrupting the normal

functionality of a MANET. Active attacks can be classified into three groups such as integrity, masquerade and tampering attacks. The general taxonomy of security attack against MANET are passive attacks such as Eavesdropping, traffic analysis, monitoring and active attacks such as Jamming, spoofing, modification, replaying, Denial of Service.

II. RELATED WORK

The various ad-hoc protocols are studied extensively in wireless network in MANET , deals with the secure and privacy issues for transmitting the packet in the wireless network with high confendiality

1. Yao-Nan Lien et al[6] proposed a new TCP congestion control mechanisms by router-assisted approach. Their proposed TCP-protocol, called TCP Muzha uses the assistance provided by routers to achieve better congestion control. To use TCP Muzha, routers are required to provide some information allowing the sender to estimate more accurately the remaining capacity over the bottleneck node with respect to the path from the sender to the receiver With this information TCP Muzha will be able to enhance the performance of both TCP network.

2. Broch et al. [17] propose a principle that allows a DSR-based MANET with single gateway to span across heterogeneous link layers. This architecture supports only a single gateway in a MANET IP subnet.

3. Manickam Gunasekaran et.al proposed architecture is designed based on the k-times anonymous authentication and onion routing - a cryptography concept which supports for anonymous communication. The simulation results prove the necessity and effectiveness of the proposed architecture in achieving such privacy and security in the integrated environment.

III. DESIGN AND IMPLEMENTATION

A. PDM Techniques

Partition Detection method is used, because the network contains huge number of nodes/hops. It is very hard in the network if problem/failure occurs. For this, here partition the nodes based on the packet size and information/data it contains and forms a cluster in distributed network. Here each partition has routing table along with the path it traversed. Using this technique, can able to avoid message overhead, increase energy efficiency parameter, and reduce the cost of measure.

First, we should identify the problem which has occurred. If the receiver node is not receiving any acknowledgement, then it is busy with some other transaction. After receiving acknowledgement NRES to the REQ, while transacting the data, and suddenly packet transaction failed means, the allotted time for the particular transaction exceeds.

B. DBF Algorithm:

Distributed Bellman Ford algorithm is used to find the shortest path for data transmission between the nodes. In a distributed partition network, each and every node transmits the packet along the route. The route is selected using DBF algorithm, sends the packet which is nearest to the sending node. The shortest path for traversing packet from A to D is 5(A->B->C->D), the shortest path

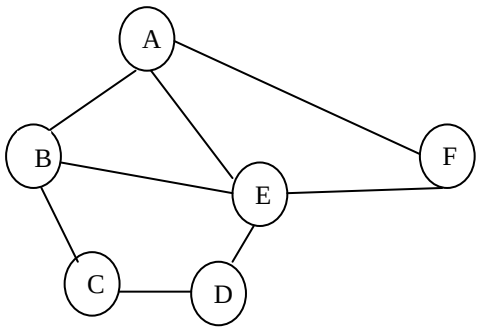

Figure 1: Distance Vector using DBF algorithm

In the figure 1, A,B,C,D,E,F are routers that is represented in the table as i. Distance between the routers are calculated using the parameter D(i,j) and Distance from the router to the neighbor is calculated using d(i,j).

$D(i,j) = \min \{d(i,k) + D(k,j)\}$ for all i<>j Here, 'k' is the neighbor

To calculate the distance from B to F,

D(B,F) = min {d(B,k) + D(k,F)., where k=A,C,E(neighbors of B(Router))

- First should find the shortest distance from the source and target using single link (i.e)D(i,j)[1]
- Next find the shortest distance from the nodes(i,j) using double link (i.e) D(i,j)[2]=min{d(i,j)+D(i,j)[1]}
- Last , find the best (h+1 or fewer)-hop path between nodes i and j , and neighbor link connected with a (h or fewer)-hop path from neighbor to j (i.e)D(i,j)[h+1] = min {d(i,k) + D(k,j)[h]}

By using this algorithm, each router maintains a separate distance table . The distance table contains the parameters like cost [D(i,k)], distance of the router ,neighbors (k1,k2…kn)

Table 1: Calculate the Shortest distance between the hops D(i,j)

Cost D(B,j)h	**Neighboring Hops**		
	k1	**k2**	**k3**
B->F	A	C	E
A->E	B	F	D

From the above distance table can easily maintain a routing table for each router. In the routing table, it contains the cost of the distance and it is measured by using the hops it crossed (i.e) either single link, double link or multiple link. Based on the cost, the router selects the next node to traverse the packet.

Table 2: Calculate the Cost of the Router

Neighboring Hops		
Destination	**Outgoing links**	**Cost**
F	k2	1
E	k3	1

Routing table is maintained by the sink node. If the node fails, then there is no acknowledgment received from the RREQ node.So that the sender can easily identify the node failure

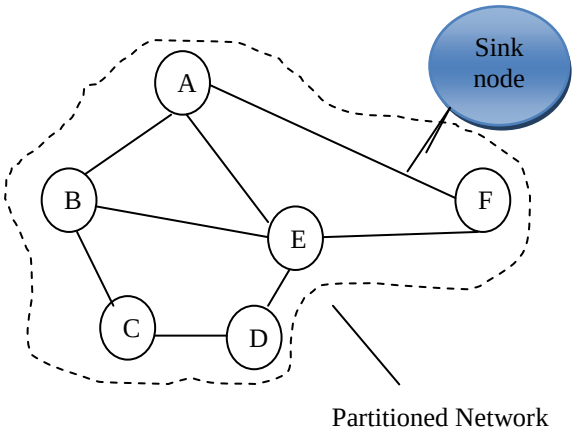

Figure 2: Partitioned Network with Sink node and Routing table

. Every node receives the request and send acknowledgement to the sender node, so that node is in ready state to receive the packet. The status of each packet transaction is recorded by the router in the router table in sink node.In the above figure 2, the partitioned network is shown by using dotted lines, the 6 nodes which are partitioned as a single network, based on the split up can easily found the shortest distance, easy to recover the packet loss.

C. Time To Live (TTL)

Before transmitting the each packet in the network, the time is set to every packet, so that it can avoid congestion occurring in the network and data failure. If a packet takes more time, then it fails, and allows other packet to traversing the network. Packet contains limited information and time limit sets depends on the data that contains in packet, it will reduce the time, waiting time of each packet and congestion occurs. It will increase the speed, energy efficient and power consumption, and it can be able to transmit more packets along the network.

Time-to-live (TTL) is a value in an Internet Protocol (IP) packet that tells a network router whether or not the packet has been in the network too long and should be discarded. For a number of reasons, packets may not get delivered to their destination in a reasonable length of time. The problem of an existing work is the combination of incorrect routing tables could cause a packet to loop endlessly.

The solution for this is to discard the packet after a certain time and send a message to the originator, who can decide whether to resend the packet. The initial TTL value is set, usually by a system default, in an 8-binary digit field of the packet header. The original idea of TTL was that it would specify a certain time span in seconds that, when exhausted, would cause the packet to be discarded. Since each router is required to reduce at least one count from the TTL field, the count is usually used to mean the number of router hops the packet is allowed before it must be discarded. Each router that receives a packet reduced count. (i.e) one from the count in the TTL field.

The router table maintains the information about the packet status (i.e) it contains the details of received packet, destroyed packet. Sink node is acting like a gateway for all the partitioned network and it monitors the router table and sends the in. It is responsible for reduced power consumption during data transmission between sensors.

Beacon frame is used to monitor the node location secretly and identifies where the problem occurred and maintains the status of hop in the routing table. If problem occurs, send it to the sink node and sink node will send to the server, so that the status are recorded and cleared. It contains the information about the source that the packet sends and the destination, where the packet receives. The time which the packet travels to the next hop, if the time period exceeds then the router monitors the packet loss and update in the table. So that the sink node will update the status in the server.

D. SPPDT:

The Secure Privacy Preserving Data Transmission in MANET (SPPDT) protocol is designed to provide security and privacy for the nodes during data transmission.

1. Sneha George, Devapriya et.al[7]: an efficient privacy preserving unobservable routing method against DOS attacks for adhoc network is presented. A meaningful packet cannot be distinguished from the other packets by an outside eavesdropper.

MANET plays major role in wireless networks, because MANET carries huge number of mobile nodes in the network, produces topological changes and broadcast paradigm for secure transmission, consider the situation, when the data is communicated within the MANET, requires high degree of security in wireless network.

2. Jyothi Thalor et.al: MANET are self organizing and adaptive network that can be formed and deformed on the fly without the need of any centralized administration.

In an existing work, DSDV protocol is used for privacy packet transmission in the network, but it have some limitations when transmiting the packet (i.e) wastage of bandwidth, doesnot support Multipath Routing, difficult to determine the time delay.Zone Routing Protocol(ZRP) will only consider packet transmission within the zone is efficient. if the packet transmission is beyond the zone , then the efficient is reduced as expected.

In order to overcome the limitations of an existing protocol in the wireless network, we propose SPPDT protocol. Using this protocol, can achieve the following three factors.While transmitting a packet/data in the network, the router table checks the where the nodes comes from (Sender) and destination address. Between the transactions there are so many parameters it has to check they are:

Time to live (time perior given for that particular packet for transmission)

Shortest distance (find the next hop which is nearest to the transmitting node)

ACK (for more security, the hop has to wait until receives acknowledgement from the receiver, after ACK it sends the request to the server for packet transmission)

If time period exceeds, then the packet **backoff** and allow transmitting next packets and finally formatting the packet before reach the destination.

The advantages of this protocol includes, it will reduce the power consumption by using TTL technique (i.e., in less time many data are communicated in MANET). The following metrics are achieved using the SPPDT protocol:

1. ***Recovery Delay*** is fast when compared with other technique i.e., measure the TTL to find and establish the alternate route to sink node.
2. Increase the ***energy efficiency*** to extend the nodes lifetime in the network.
3. ***Distance*** travelled is achieved using the DBF algorithm, for the shortest path data transmission.
4. ***Message Overhead*** is reduced using distributed partition.

These metrics are used to measure the data transmission between the nodes and prevent from attackers by using Beacon frame and acknowledgement signal.

In the existing key establishment algorithm is used. It is difficult to maintain a group of key in network. In order to reduce the burden of the server, consider only requested acknowledgement only.

Recover Delay is achieved by fixing the time period for every node in the network, so that the packets are communicated as faster when compared to normal packet transmission. Here, avoid the congestion and long time waiting of packets.

Distance travelled is achieved, by clustering the network into several partition, so that thousands of nodes can be used in the network and easy to find the shortest path within the clustered environment, so that achieve large number of nodes.

In our proposed method, energy efficiency is increased for packet transmitting in ad hoc network.

There is no bandwidth wastage in our proposed method, because each and every node is monitored by the sink node and there are no excess nodes in the network, unused node in the network.

III. CONCLUSION

SPPDT is designed to address the security factors and issues in MANET. This protocol is well designed for large networks. If the number of nodes exceeds the threshold in the network, energy consumption of the node is high by achieving scalability factors of the network. Our distributed method may maintain the information of each node to the sink node. It maintains routing table and node status/failure table. The proposed protocol achieves recovery delay, energy efficiency, reduced message overhead and accuracy when compared to all existing method.

IV. REFERENCE

1. Muthumanikam Gunasekaran and Kandaswamy Premalatha " SPAWN: A Secure Privacy-Preserving Architecture in Wireless Mobile Adhoc Networks" EURASIP Journal on Wireless Communication and Networking, SPRINGER Open Journal.2013
2. S.Jayamoorthy, I.Varalakshmi, S.Kumarakrishnan "Monitoring and Self-Transmitting Data Using Zone Routing Protocol in Ad-hoc Network towards Effective Mobility Management" International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 4, April 2014, pg.269 – 274.2014
3. Shalini.S, K.Ramalakshmi, P.Anitha Christy Angelin "A Survey on Partition and Recovery Methods of Node Failure in Wireless Sensor Networks"International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 12. Dec 2013.
4. Yih-Chun Hu and Adrian Perrig, "A survey of secure wireless ad hoc routing" *IEEE Security and Privacy*, 2(3):28–39, 2004
5. Gene Tsudik - Professor at the School of Information and Computer Science, "SPROUT-Security and Privacy in Location-based MANETs/VANETs **"**University of California Irvin
6. http://www.academia.edu/1283540/Simulation_of_Ad-hoc_Networks_Using_DSDV_AODV_And_DSR_Protocols_And_Their_Performance_Comparison
7. Sneha George, Devapriya "privacy preserving unobservable routing method against DOS attacks for adhoc network"